UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/791,414	03/03/2004	Jing Xiang	NRT.0124US	2562

21906 7590 08/09/2007

TROP PRUNER & HU, PC
1616 S. VOSS ROAD, SUITE 750
HOUSTON, TX 77057-2631

EXAMINER	
TABOR, AMARE F	

ART UNIT	PAPER NUMBER
2109	

MAIL DATE	DELIVERY MODE
08/09/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

80

Office Action Summary	Application No.	Applicant(s)	
	10/791,414	XIANG ET AL.	
	Examiner	Art Unit	
	Amare F. Tabor	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *03/03/04 and 10/25/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-19 are examined.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim is 8 rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 8 recite the limitation "at least one ***signal*** in at least one ***carrier wave*** for transmitting a computer program"; thus, the claims do not constitute statutory subject matter.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-19 are rejected under 35 U.S.C. 102(b) as being anticipated by "***Ahonen***" (US Pub No.: 2001/0009025 A1).

4. *As per claims 1, 3 and 4*, Ahonen discloses,

A method for maintaining secure network connections, the method comprising: (Par. [0004], lines 2-4, "there is provided a secure communication method for allowing a mobile host to communicate with a correspondent host over a Virtual Private Network via a Security Gateway (SG)").

- detecting a change of address associated with a first network element; wherein the secure message comprises information associated with the change of address; (Par. [0129], 1-5, "if the source IP address was changed, the firewall 3 will also forward the new Source and Destination IP addresses to the correspondent host 4, which identifies the appropriate SA via ISAKMP Cookies, IPsec protocol ID, and SPI number, which are also attached to the message").

- updating at least one second security configuration at the second network element based at least in part on the at least one secure message; (Par. [0008], "wherein said data packets are forwarded by the SG to the correspondent host only if they are authenticated by the SG")

- updating at least one first security configuration at the first network element; (Par. [0010], "preferably, the authentication certificate sent to the SG contains an IP address of the mobile host. This may be required, for example, when the mobile host has been allocated a new IP address").

- transmitting at least one secure message from the first network element to a second network element (Par. [0007], "sending data packets from the mobile host to the correspondent host using the identified SA, via the SG")

5. As per claim 2, Ahonen discloses,

- wherein a lookup of security associations is not dependent on any destination address (Par. [0012], "embodiments of the present invention reduce the amount of security related messaging during on-the-fly IP address changes, as the SAs needed to provide for secure communication between the mobile host and the correspondent host pre-exist. When it is required to initiate a new communication, it is only necessary for the mobile host to authorise the SG to forward packets belonging to a certain SA between the mobile host and said correspondent host").

6. As per claim 5 and 6, Ahonen discloses,

- wherein communications between the first network element and the second network element are based on a security architecture for the internet protocol (IPsec); and at least part of the communications between the first network element and the second network element are based on an internet security association and key management protocol (ISAKMP) (see Figure 2 & Par. [0048], lines 4-10, "firstly, a single ISAKMP Security Association (SA) is negotiated between the **mobile** host 1 and the firewall 3. The ISAKMP SA provides protection for the IKE messaging itself. Secondly, several pairs (or in the case of a highly memory limited device only a single pair) of IPsec Security Associations (SA) are established for the purpose of protecting actual user data traffic").

7. As per claim 7, Ahonen discloses,

- wherein the second network element identifies at least one security association based on at least one cookie field in the at least one secure message (Par. [0055], lines 1-3, "it is noted that the ISAKMP uses the Initiator and responder cookie fields in the ISAKMP header to identify the particular ISAKMP SAs for itself").

8. As per claims 8 and 9, Ahonen discloses,

At least one processor readable carrier for storing and transmitting a computer program of instructions configured to be readable by at least one processor for instructing the at least one processor to execute a computer process for performing the method as recited in claim 1 (Par. [0106], lines 1-4, "the contents of the received certificates are stored in a nominal (secure) database, referred to here as a Remote Control Database (RCDB), within firewall 3"); and (Figure 1 & Par. [0023], "means for forwarding the data packets from the SG to said correspondent host providing that the received data packets are authenticated").

9. As per claim 10, Ahonen discloses,

A method for maintaining secure network connections, the method comprising: (rejection of claim 1 above is applied to this limitation)

- duplicating, between a second network element and a third network element, information associated with a secure network connection between a first network element and the second network element; and replacing the second network element with the third network element in the secure network connection with the first network element; (Par. [0096], lines 1-6, "the result of this process is that SAs (phase 1 and phase 2) are established between the mobile host 1 and the firewall 3, and between the mobile host 1 and the correspondent host 4. It will be appreciated that the mobile host may additionally establish SAs with a second (or subsequent) correspondent host").

wherein a lookup of security associations associated with the secure network connection is not dependent on any destination address; (rejection of claim 2 above is applied to this limitation)

10. As per claim 11, Ahonen discloses,

- sending at least one secure message from the third network element to the first network element (Par. [0037], "a continuous channel method (REKEY) to always maintain at least one valid phase 1 Security Association (SA) between the mobile host 1 and the firewall 3 and also between the mobile host 1 and the correspondent host 4").

11. As per claim 12, Ahonen discloses,

A method for maintaining secure network connections, the method comprising: (rejection of claim 1 above is applied to this limitation)

- configuring a plurality of security gateways such that a lookup of security associations is not dependent on any destination address; and sharing at least one security association among the plurality of security gateways (Par. [0035], lines 6-12; see Figure 1 and rejection of claim 2 above is applied to this limitation).

12. *As per claims 13, 15 and 16*, Ahonen discloses,

A system for maintaining secure network connections, the system comprising: (Par. [0019], lines 2-4, "provided a Security Gateway (SG) of Virtual Private Network, the SG enabling secure communication between a mobile host and a correspondent host).

- means for detecting a change of address associated with a first network element; wherein the secure message comprises information associated with the change of address; (Par. [0129], 1-5, "if the source IP address was changed, the firewall 3 will also forward the new Source and Destination IP addresses to the correspondent host 4, which identifies the appropriate SA via ISAKMP Cookies; IPsec protocol ID, and SPI number, which are also attached to the message"); which include inherent means for detecting address change.

- means for updating at least one second security configuration at the second network element based at least in part on the at least one secure message; (Par. [0022], "means for receiving data packets sent from the mobile host and for authenticating the data packets").

- means for updating at least one first security configuration at the first network element; (Par. [0021], "means for subsequently initiating a communication between the mobile host and the SG using a negotiated SA and for receiving an authentication certificate sent from the mobile host, the certificate containing at least the identity of the mobile host and an IP address of the mobile host").

- means for transmitting at least one secure message from the first network element to a second network element (Par. [0020], "means for negotiating one or more Security Association (SAs) between the mobile host and the Security Gateway (SG)").

13. *As per claim 14*,

This claim recites similar limitation to that of claim 2; and is rejected on similar reasons as set forth the rejection of claim 2 above.

14. *As per claim 17-19*,

These claims recite similar limitation to that of claims 5-7 respectively; and are rejected on similar reasons as set forth the respective rejections of claims 5-7 above.

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO-892).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Amare F. Tabor whose telephone number is (571) 270-3155. The examiner can normally be reached on Mon-Fri 7:30a.m. to 5:00p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Chameli Das can be reached on (571) 272-3696. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AFT

JEAN M. CORRIELUS
PRIMARY EXAMINER
Art Unit 2162
Date: 8/3/07